

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-18148

(P2003-18148A)

(43) 公開日 平成15年1月17日 (2003.1.17)

(51) IntCl. ⁷	識別記号	F I	テーマコード(参考)
H 0 4 L	9/08	H 0 4 L 9/00	6 0 1 C 5 J 1 0 4
H 0 4 B	7/26	H 0 4 B 7/26	M 5 K 0 0 2
	10/00	9/00	A 5 K 0 6 7
	10/22	H 0 4 L 9/00	6 7 5 A
H 0 4 L	9/32	H 0 4 B 7/26	1 0 9 R

審査請求 有 請求項の数12 O L (全 7 頁) 最終頁に続く

(21) 出願番号 特願2001-204889(P2001-204889)

(22) 出願日 平成13年7月5日(2001.7.5)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 木下 雄弘

東京都青梅市末広町2丁目9番地 株式会
社東芝青梅工場内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

Fターム(参考) 5J104 AA03 AA16 EA04 EA21 NA02
PA02

5K002 AA05 DA05 FA03 GA07

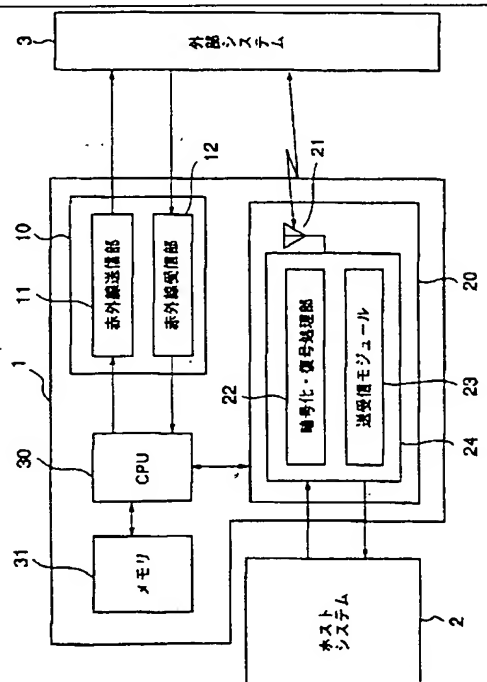
5K067 AA33 BB21 EE35 EE37 HH36

(54) 【発明の名称】 無線データ通信装置及びそのデータ通信方法

(57) 【要約】

【課題】 共有鍵方式のセキュリティ機能に必要なキー情報の秘匿性を十分に確保できる無線データ通信装置を提供することにある。

【解決手段】 Bluetooth無線通信方式を採用する無線データ通信装置において、認証処理や暗号化処理に使用する共有キー情報を赤外線通信部10を使用して交換する。CPU30は、交換した共有キー情報をメモリ31に記憶し、認証処理及び暗号化・復号化処理部22の暗号化・復号化キー情報の生成処理に使用する。無線データ通信部20は、暗号化・復号化処理部22により暗号化されたデータを送信し、また受信データの復号化を実行する。



【特許請求の範囲】

【請求項 1】 データの暗号化処理を実行する暗号化手段と、

相手局との間で暗号化データの送受信を行なう無線データ通信手段と、

前記暗号化手段での暗号化処理に必要なキー情報を前記相手局との間で交換するキー情報通信手段とを具備したことを特徴とする無線データ通信装置。

【請求項 2】 前記キー情報通信手段は、赤外線通信方式によりデータ通信を実行する赤外線通信手段であることを特徴とする請求項 1 記載の無線データ通信装置。

【請求項 3】 前記無線データ通信手段を使用して、データ通信を行なう相手局との接続に必要な手順を実行する手段を有することを特徴とする請求項 1 または請求項 2 のいずれか 1 項に記載の無線データ通信装置。

【請求項 4】 前記キー情報通信手段で交換したキー情報を登録し、当該キー情報を使用してデータ通信を行なう相手局の認証処理を実行する手段を有することを特徴とする請求項 1 から請求項 3 のいずれか 1 項に記載の無線データ通信装置。

【請求項 5】 前記キー情報通信手段は、前記無線データ通信手段とは異なる無線通信方式によるデータ通信を実行する無線通信手段であることを特徴とする請求項 1 記載の無線データ通信装置。

【請求項 6】 電子機器に設けられる回路モジュールであって、

前記電子機器で処理されるデータの暗号化処理を実行する暗号化モジュールと、

相手局との間で暗号化データの送受信を行なう無線データ通信モジュールと、

前記無線データ通信モジュールとは異なる無線通信方式により、前記暗号化モジュールでの暗号化処理に必要なキー情報を相手局との間で交換する通信モジュールとを具備したことを特徴とする回路モジュール。

【請求項 7】 前記通信モジュールは、赤外線通信モジュールから構成されていることを特徴とする請求項 6 記載の回路モジュール。

【請求項 8】 前記通信モジュールは、セルラー電話モジュールから構成されていることを特徴とする請求項 6 記載の回路モジュール。

【請求項 9】 前記電子機器に対して着脱自在なカードモジュールから構成されていることを特徴とする請求項 6 から請求項 8 のいずれか 1 項に記載の回路モジュール。

【請求項 10】 前記通信モジュールで交換したキー情報を登録し、当該キー情報を使用してデータ通信を行なう相手局の認証処理を実行する手段を有することを特徴とする請求項 6 から請求項 9 のいずれか 1 項に記載の回路モジュール。

【請求項 11】 データ通信を行なうための無線データ

通信装置に適用するデータ通信方法であって、

相手局との間で、データの暗号化処理に必要なキー情報を赤外線通信手段により交換するステップと、

前記キー情報を使用してデータの暗号化処理を実行するステップと、

暗号化データの送受信を無線データ通信手段により実行するステップとを有することを特徴とする無線データ通信装置。

【請求項 12】 前記無線データ通信手段を使用して、データ通信を行なう相手局との接続に必要な手順を実行するステップと、

前記赤外線通信手段で交換したキー情報を登録し、当該キー情報を使用してデータ通信を行なう相手局の認証処理を実行するステップとをさらに有することを特徴とする請求項 11 記載のデータ通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、一般的には無線データ通信装置に関し、特にセキュリティ技術の改善に関する。

【0002】

【従来の技術】 近年、各種の電子機器の間で、例えば Bluetooth と呼ばれる無線通信方式による近距離のデータ通信を可能とする技術が開発されている。各種の電子機器としては、パーソナルコンピュータ以外に、例えば PDA (Personal Digital Assistant) と呼ばれる携帯情報端末、セルラー電話機 (携帯電話機)、携帯型オーディオ機器、あるいはデジタルカメラなどが含まれる。

【0003】 これらの電子機器間で、無線データ通信が可能であれば、ケーブルによる接続が不要になるなどの利便性を向上できる。このような機能を実現するために、電子機器に対して着脱可能な IC カードや、機器の内部に設けるチップセット (IC 回路モジュール) から構成される無線データ通信装置 (無線通信デバイス) が開発されている。

【0004】 ところで、無線データ通信では、相手局 (無線通信デバイスを含む相手側電子機器) との間で交換するデータを保護するためのセキュリティ機能が重要である。例えば Bluetooth 無線通信方式では、セキュリティ機能として、認証機能と暗号化 (復号化を含む) 機能の規格が提案されている。いずれの機能も、共有鍵方式と呼ばれる鍵情報 (以下キー情報と呼ぶ) の交換を伴う方式が採用されている。即ち、特定の相手局との接続の可否を判断する認証処理、及び通信中のデータを第三者から保護するための暗号化処理のいずれの場合でも、共有するキー情報を使用するセキュリティ方式である。

【0005】

【発明が解決しようとする課題】 例えば Bluetooth

無線通信方式を採用した無線データ通信では、相手局との間でキー情報を共有（交換）し、当該キー情報を使用して認証処理や暗号化処理を行なうセキュリティ方式が採用されている。

【0006】Bluetooth無線通信方式では、セキュリティ機能は、リンクキー（link key）という概念により管理されている。リンクキーは、ある特定の通信端末間のセキュリティを管理するパラメータ情報であり、データベースに登録されて使用される。このリンクキー（即ち、キー情報）の秘匿性が、無線データ通信におけるセキュリティ機能の強度に大きく影響する。要するに、無線データ通信を開始する際に、セキュリティ機能に必要なキー情報を第三者から確実に保護することが必要である。しかしながら、従来では、相手局と共有するキー情報を無線通信により交換する方式が採用されているため、秘匿性の確保が必ずしも十分とはいえない。

【0007】そこで、本発明の目的は、共有鍵方式のセキュリティ機能に必要なキー情報の秘匿性を十分に確保できる無線データ通信装置を提供することにある。

【0008】

【課題を解決するための手段】本発明は、例えばBluetooth無線通信方式を採用する無線データ通信装置において、共有キー情報を使用して認証処理や暗号化処理を行なうセキュリティ方式に関し、通常データ通信（ユーザデータの通信）に使用する無線通信規格とは異なる無線通信方式により、当該共有キー情報の通信を実行する無線データ通信装置である。

【0009】具体的には、本発明の装置は、データの暗号化処理を実行する暗号化手段と、相手局との間で暗号化データの送受信を行なう無線データ通信手段と、暗号化手段での暗号化処理に必要なキー情報を相手局との間で交換するキー情報通信手段とを備えたものである。当該キー情報通信手段は、無線データ通信手段の無線通信規格とは異なる無線通信方式であり、具体的には赤外線通信方式を採用した通信手段である。

【0010】このような構成により、無線データ通信手段によるデータ通信を実行する前段階のセキュリティ手順として、相手局との間でキー情報を共有するために、当該キー情報を赤外線通信方式等のキー情報通信手段により交換する。換言すれば、通常データ通信方式と、セキュリティ機能に必要なキー情報の通信方式とを分離する。これにより、同一の通信方式による通信と比較して、通信中のキー情報の秘匿性を十分に確保することが可能となる。従って、共有するキー情報を使用するセキュリティ機能の強度を向上させることができるため、結果としてデータ通信の信頼性を向上させることが可能となる。

【0011】

【発明の実施の形態】以下図面を参照して、本発明の実施の形態を説明する。

【0012】（無線データ通信装置及びシステムの構成）図1は、同実施形態に関する無線データ通信装置及び通信システムの構成を示すブロック図である。

【0013】同実施形態では、無線データ通信装置（以下無線通信デバイスと表記する）1は、PDAなどの情報端末等の電子機器を意味するホストシステム2に対して着脱可能なICカード、または当該システム2に内蔵されるチップセットIC（回路モジュール）から構成される。更に、同実施形態では、ホストシステム2が、当該無線通信デバイス1を介して、外部システム（以下相手局と表記する）3との間でデータ通信を行なう通信システムを想定する。ここで、相手局3とは、当該無線通信デバイス1と同様の仕様のデバイスを有する電子機器である。

【0014】無線通信デバイス1は、メイン要素である無線データ通信部20とは別に、キー情報交換部として機能する赤外線通信部10を有する。赤外線通信部10は、通常のIrDA（Infrared Data Association）規格による赤外線データ通信を実行するモジュールであり、赤外線送信部11と赤外線受信部12とから構成されている。

【0015】無線データ通信部20、マイクロプロセッサ（CPU）30、及びメモリ31は、Bluetooth無線通信方式によるデータ通信機能を実現するモジュールである。無線データ通信部20は、大別して送受信用のアンテナ21と、暗号化・復号化処理部22と、送受信モジュール23とを有する。送受信モジュール23は、無線データ通信機能を実現するために、無線通信コントローラ、高周波処理部、ベースバンド処理部、及びI/O処理部等の要素を有する。暗号化・復号化処理部22は、Bluetooth無線通信方式でのキー情報（リンクキー）を使用して、送信データの暗号化処理及び受信データの復号化処理を実行するモジュールである。

【0016】CPU30は、Bluetooth無線通信方式によるデータ通信及びセキュリティ処理の制御を実行する。メモリ31は、セキュリティ処理におけるキー情報（リンクキー）を記憶する例えばフラッシュEEPROMからなる。

【0017】（システムの概略的動作）以下図4のフローチャート及び図7のタイミングチャートを参照して、同実施形態の無線通信デバイス1によるデータ通信システムの概略的動作を説明する。

【0018】まず、CPU30は、ホストシステム2からの指示に従って、無線データ通信部20を起動して、自局と相手局3間のデータ通信を行なうための一連の手順（詳細は後述する）を実行する（ステップS21）。具体的には、無線データ通信部20のアンテナ21及び送受信モジュール23により、相手局3と交信して、キー情報の交換に必要な赤外線通信部10に相当する通信

手段を備えているか否かを確認する(ステップS2)。即ち、図7の70に示すように、相手局3の属性に含まれる赤外線通信部10に相当する通信機能を備えているか否かを問い合わせる。自局側であるCPU30は、相手局3からの回答により、赤外線通信部10に相当する通信手段を備えていることを確認する(71)。

【0019】CPU30は、赤外線通信部10の赤外線送信部11及び赤外線受信部12を通じて、図7の72に示すように、相手局3との間でセキュリティ機能に必要なキー情報(後述するリンクキー)を交換する(ステップS23)。CPU30は、交換(共有)したキー情報をメモリ31に記憶(データベースへの登録)する(ステップS24)。

【0020】次に、CPU30は、ホストシステム2からのデータ通信要求に応じて、メモリ31からキー情報を読出して、暗号化・復号化処理部22に引き渡す。暗号化・復号化処理部22は、キー情報を使用して、ホストシステム2からの送信データを暗号化処理して送受信モジュール23に転送する(ステップS25)。ここで、図7の73及び74に示すように、自局と相手局3のそれぞれは、交換したキー情報を使用して、相互の認証処理及び暗号化・復号化に必要なキー情報の生成処理を実行する。

【0021】暗号化・復号化処理部22は、生成したキー情報を使用して、送信データの暗号化及び受信データの復号化の処理を実行する。これにより、自局と相手局3間は、図7の75に示すように、暗号化データの通信を行なう。即ち、送受信モジュール23は、暗号化データをアンテナ21を介して相手局3に送信する。また、暗号化・復号化処理部22は、キー情報を使用して、送受信モジュール23により相手局3からの受信データを復号化処理してホストシステム2に転送する(ステップS25)。

【0022】(セキュリティ機能を有するデータ通信動作)以下図2及び図3のフローチャートを参照して、同実施形態の無線通信デバイス1において、特にBluetooth無線通信方式によるデータ通信及びセキュリティ処理の手順を説明する。

【0023】Bluetooth無線通信方式でのセキュリティ方式は、データ通信の接続要求に応じて、リンクキー(キー情報)を使用して認証処理を実行し、認証された場合に当該リンクキーを使用して暗号化・復号化処理に必要なキー情報を生成する手順を実行する(図3のフローチャートを参照)。

【0024】同実施形態では、当該セキュリティ手順の前段階として、CPU30は、赤外線通信部10を使用して、相手局3との間でキー情報を交換(共有)する処理を実行する。ここで、CPU30は、Bluetooth規格に含まれるSDP(Service Discovery Protocol)による問い合わせ処理(SDP-Service Search Reque

st)を利用して、相手局3の属性に含まれる赤外線通信部10に相当する通信機能を備えているか否かを確認する(ステップS1)。

【0025】CPU30は、無線データ通信部20のアンテナ21及び送受信モジュール23を介して相手局3にSDPによる問い合わせを実行し、相手局3からの問い合わせ応答を待つ(ステップS2)。具体的には、相手局3は、赤外線通信部10に相当する通信機能を備えているという属性を示すパケット(SDP-Service Search Response)を送信する。CPU30は、相手局3からの問い合わせ応答により、赤外線通信部10によるデータ通信が可能であることを確認する(ステップS3のYES)。次に、CPU30は、赤外線送信部11を通じて呼び出し処理(page)を実行することにより、相手局3との通信接続の確立を図る(ステップS4)。具体的には、CPU30は、IDパケットを送信し、相手局3からの呼び出し応答(page response)を赤外線受信部12を通じて受信すると、通信接続フェーズへ移行する(ステップS5のYES)。

【0026】このような相手局3との通信により、CPU30は、相手局3との間で赤外線通信部10によるデータ通信接続を確立し、セキュリティ機能に必要なキー情報の交換(共有)を実行し、メモリ31に記憶する(図4のフローチャートを参照)。

【0027】次に、図3のフローチャートを参照して、同実施形態のセキュリティ手順を説明する。

【0028】まず、Bluetooth方式のセキュリティ手順としては、リンクキーの登録がなされているか否かが判断される(ステップS10)。同実施形態では、相手局3との間で赤外線通信部10により交換したキー情報をリンクキーとして利用する。即ち、CPU30は、メモリ31に記憶されているキー情報を、データベースに登録されたリンクキーとして利用する。

【0029】なお、通常のBluetooth方式のセキュリティ手順として、初期時には、リンクキーはデータベースには登録されていないため、初期化キーと称する暫定リンクキーの生成処理が実行される(ステップS10のNO)。初期時には、当該初期化キーによる認証処理が実行される。この初期キーの生成では、各端末

(電子機器)で個別に入力されるPINコードと、内部で発生される乱数データとがパラメータとして使用される。この乱数データは、相互に通信されて共有される。

【0030】CPU30は、データベースに登録されているリンクキーとして、メモリ31に記憶された共有キー情報を利用して、相手局3の認証処理を実行する(ステップS11)。この認証処理により確認されると、CPU30は、当該リンクキー(共有キー情報)を使用して、暗号化・復号化キー情報を生成し、暗号化・復号化処理部22に引き渡す(ステップS13)。

【0031】ホストシステム2からデータ送信の要求が

あると、暗号化・復号化処理部22は、暗号化・復号化キー情報を使用して、ホストシステム2からの送信データを暗号化処理する(ステップS14のYES, S15)。送受信モジュール23は、暗号化データをアンテナ21を介して相手局3に送信する(ステップS16)。

【0032】一方、送受信モジュール23が相手局3からデータを受信すると、暗号化・復号化処理部22は、暗号化・復号化キー情報を使用して受信データを復号化処理する(ステップS17, S18)。暗号化・復号化処理部22は、復号化した受信データをホストシステム2に転送する。

【0033】以上のように同実施形態の無線データ通信方式によれば、データ通信を実行する前段階のセキュリティ手順として、相手局との間でセキュリティ機能に必要なキー情報(リンクキーとして利用)を共有するために、当該キー情報を赤外線通信部10により交換する。要するに、通常のデータ通信とは異なる無線通信方式により、セキュリティ機能に必要なキー情報の通信を行なう。従って、無線データ通信部20を使用する通信方式と比較して、通信中のキー情報の秘匿性を十分に確保することが可能となる。従って、共有するキー情報を使用するセキュリティ機能の強度を向上させることができるため、結果としてデータ通信の信頼性を向上させることが可能となる。

【0034】(変形例)図5及び図6は、同実施形態の変形例に関する図である。

【0035】本変形例は、図5に示すように、キー情報交換部として、赤外線通信部10の代わりに、セルラー電話装置(携帯電話機)50を利用する無線データ通信装置1である。要するに、キー情報交換部は、無線データ通信部20と異なる無線通信方式の通信装置である。

【0036】本変形例の場合でも、赤外線通信部10の代わりにセルラー電話装置50を利用する点が異なるだけで、基本的な動作は同実施形態と同様である。即ち、図6のフローチャートに示すように、セキュリティ手順の前段階として、CPU30は、セルラー電話装置50を使用して、相手局3との間でキー情報を、前述したSDPによる問い合わせ処理を利用して、相手局3の属性に含まれるセルラー電話通信機能を備えているか否かを確認する(ステップS60)。CPU30は、相手局3からの問い合わせ応答により、セルラー電話装置50によるデータ通信が可能であることを確認する(ステップS61, S62)。次に、CPU30は、セルラー電話装置50を通じて呼び出し処理を実行することにより、相手局3との通信接続の確立を図る(ステップS63)。具体的には、CPU30は、IDパケットを送信

し、相手局3からの呼び出し応答をセルラー電話装置50を通じて受信すると、通信接続フェーズへ移行する(ステップS64のYES)。

【0037】なお、図5に示すセルラー電話装置50以外の各構成要素は、図1に示す同一符号の構成要素の機能と同様である。また、セキュリティ処理の手順は、同実施形態の図3のフローチャートで示すものと同様である。

【0038】

【発明の効果】以上詳述したように本発明によれば、共有鍵方式のセキュリティ機能に必要なキー情報を、通常のデータ通信(ユーザデータの通信)に使用する無線通信規格とは異なる無線通信方式により交換する。従って、通信中のキー情報の秘匿性を十分に確保できる。これにより、共有するキー情報を使用するセキュリティ機能の強度を向上させることができるため、結果として信頼性の高い無線データ通信機能を実現することができる。

【図面の簡単な説明】

【図1】本発明の実施形態に関する無線データ通信装置及びデータ通信システムの構成を示すブロック図。

【図2】同実施形態に関する無線データ通信装置の接続動作を説明するためのフローチャート。

【図3】同実施形態に関する無線データ通信装置のセキュリティ動作を説明するためのフローチャート。

【図4】同実施形態に関するシステムの概略的動作を説明するためのフローチャート。

【図5】同実施形態の変形例に関するブロック図。

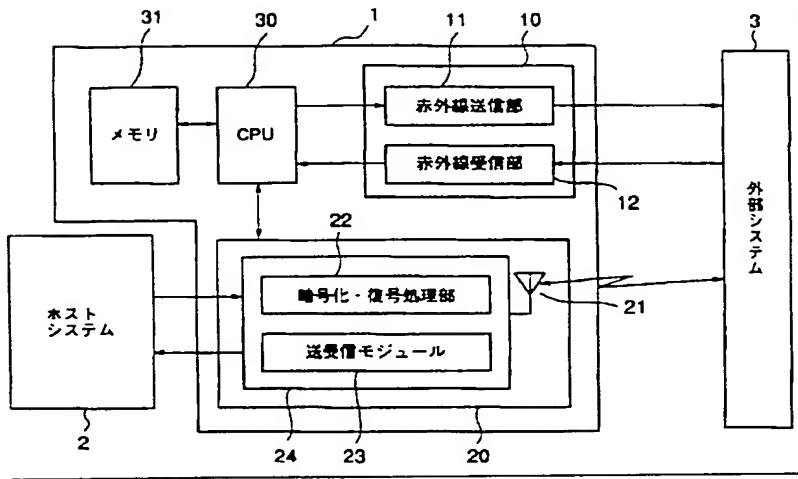
【図6】同変形例に関する無線データ通信装置の接続動作を説明するためのフローチャート。

【図7】同実施形態に関するシステムの概略的動作を説明するためのタイミングチャート。

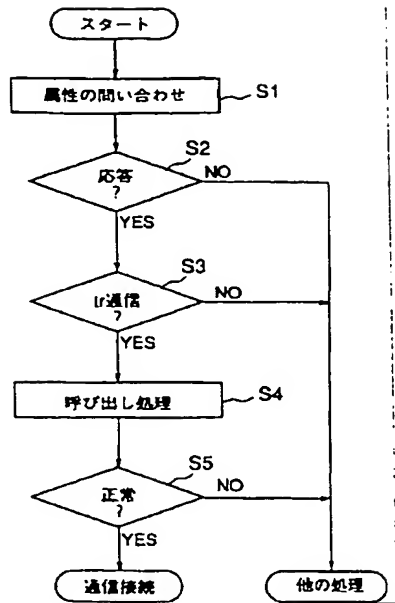
【符号の説明】

- 1…無線データ通信装置(無線通信デバイス)
- 2…ホストシステム(電子機器)
- 3…相手局(外部システム)
- 10…赤外線通信部
- 11…赤外線送信部
- 12…赤外線受信部
- 20…無線データ通信部
- 21…アンテナ
- 22…暗号化・復号化処理部
- 23…送受信モジュール
- 30…マイクロプロセッサ(CPU)
- 31…メモリ
- 50…セルラー電話装置(携帯電話機)

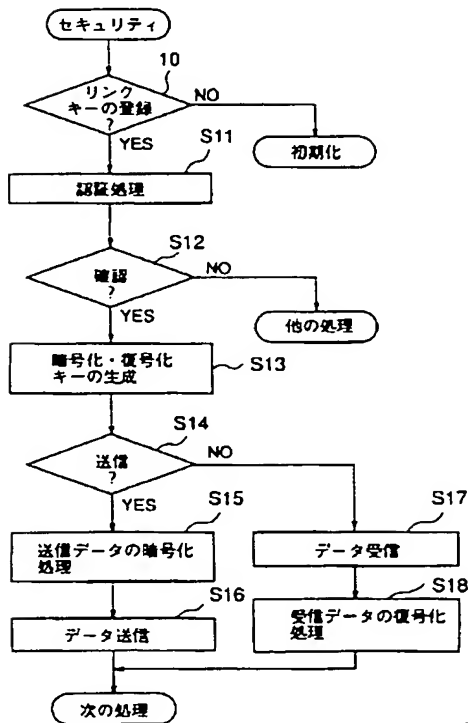
【図1】



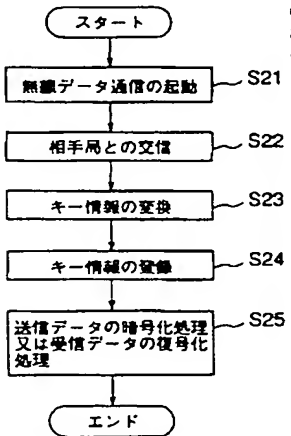
【図2】



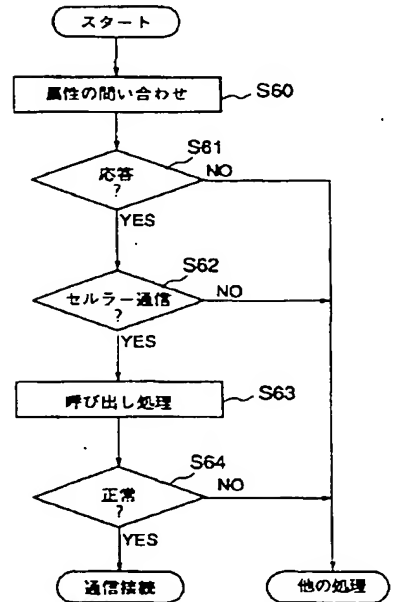
【図3】



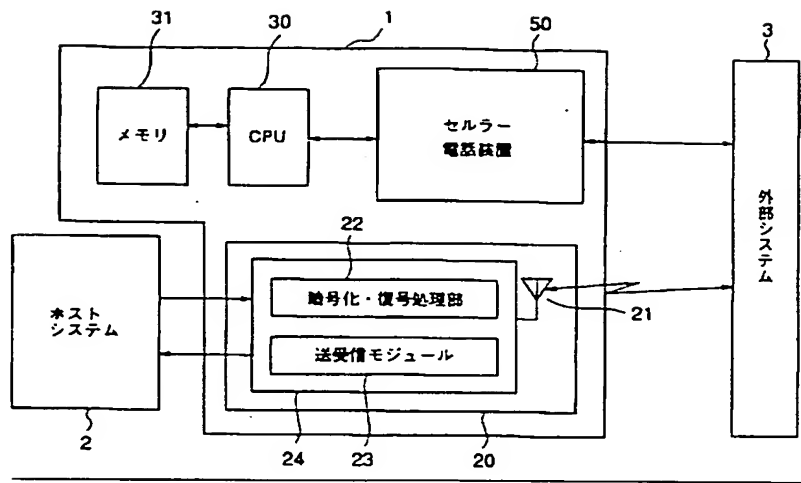
【図4】



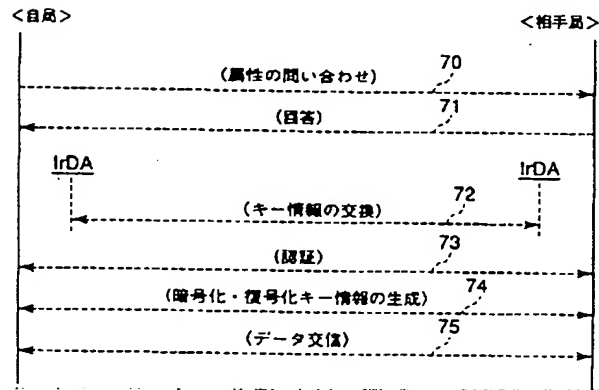
【図6】



【図5】



【図7】



フロントページの続き

(51) Int. Cl. 7

識別記号

F I

データベース(参考)

H 0 4 Q 7/38

THIS PAGE BLANK (USPTO)